Customer Master Data Protection Agreement

This Customer Master Data Protection Agreement (**"MDPA"**), forms part of the Agreement (as defined below) and applies where, and to the extent that, Cisco Processes Personal Data as a Processor for Customer when providing Products and/or Services (as defined below) under the Agreement, (each a "**Party**" and together the "**Parties**").

Unless otherwise specified in this MDPA, the terms of the Agreement shall continue in full force and effect. All capitalized terms not defined in this MDPA shall have the meanings set forth in the Agreement. Any privacy or data protection related clauses or agreement previously entered into by Cisco and Customer, with regards to the subject matter of this MDPA, shall be superseded by and replaced with this MDPA.

1. Definitions

1.1. **"Affiliates"** means, with respect to Customer, its affiliates as defined in the Agreement, and with respect to Cisco, companies within the Cisco group that may Process Customer Personal Data in order to provide the Products and/or Services. Such Affiliates include Cisco Systems, Inc., Cisco Commerce India Private Limited, Cisco Systems G.K., Cisco Systems Australia Pty Limited, Cisco Systems Canada Co., Cisco International Limited, Cisco Systems (Italy) S.R.L., Cisco Systems International B.V., ThousandEyes LLC, Broadsoft, Inc., AppDynamics LLC, AppDynamics International Ltd., Meraki LLC and Duo Security LLC. Unless otherwise explicitly agreed by the Parties, any legal entities which become part of the Cisco group of companies through an acquisition or merger are not considered Affiliates for the purposes of this MDPA.

1.2. **"Agreement"** means the written or electronic agreement between Customer and applicable Cisco entity for the provision of the Services and/or Products to Customer or any other terms where the parties expressly agree to this document (e.g.: the Cisco End User License Agreement ("**EULA**")); or where Customer has purchased a Cisco-branded Service from Cisco partner, "Agreement" means, for the purposes of this MDPA only, the applicable Service Description listed at https://www.cisco.com/c/en/us/about/legal/service-descriptions.html.

1.3. **"APEC"** means the Asia Pacific Economic Cooperation, a regional economic forum established in 1989 to leverage the growing interdependence of the Asia-Pacific. See http://www.apec.org for more information.

1.4. **"APEC Member Economy"** means the 21 members of APEC: Australia, Brunei Darussalam, Canada, Chile, China, Hong Kong-China, Indonesia, Japan, Republic of Korea, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, Philippines, Russia, Singapore, Chinese Taipei, Thailand, United States, and Vietnam.

1.5. **"Approved Jurisdiction"** means a member state of the EEA, or other jurisdiction approved as having adequate legal protections for data by the European Commission, currently found here: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

1.6. **"Cisco"** means the applicable Cisco entity that is party to the Agreement and its Affiliates.

1.7. **"CCPA"** means the California Consumer Privacy Act (Cal. Civ. Code §§ 1798.100 to 1798.199) as amended by the California Privacy Rights Act ("CPRA"), and any related regulations or guidance provided by the California Attorney General.

1.8. **"Controller"** means an entity that determines the purposes and means of the processing of Personal Data. It shall have the same meaning ascribed to "controller" under the GDPR and other equivalent terms under applicable Data Protection Laws (e.g.: "Business" as defined under the CCPA), as applicable.

1.9. **"Customer"** means the Party identified in the Agreement receiving Services and/or Products from Cisco under the Agreement**.**

1.10. **"Data Breach"** means a breach of Security Measures leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data.

1.11. **"Data Protection Laws"** means all mandatory applicable laws that apply to the Processing of Personal Data under the Agreement.

1.12. **"Data Subject"** means the individual to whom Personal Data relates (e.g.: "Consumer" as defined under the CCPA).

1.13. **"EEA"** means those countries that are members of European Free Trade Association (**"EFTA"**), and the then-current, post-accession member states of the European Union.

1.14. **"EU Standard Contractual Clauses"** means the agreement set forth in the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 for the transfer of Personal Data to Processors established in third countries which do not ensure an adequate level of data protection, as supplemented by the terms agreed in Attachment A, and any subsequent changes approved by the European Commission with an official decision.

1.15. **"GDPR"** means Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons regarding the processing of Personal Data and on the free movement of such data (General Data Protection Regulation).

1.16. **"Personal Data"** means any information about, or related to, an identifiable individual Processed by Cisco on behalf of Customer. It includes any information that can be linked to an individual or used to directly or indirectly identify an individual, natural person.

1.17. **"Privacy Data Sheet(s)"** means the applicable document located on Cisco's Trust Portal that describes the Processing activities in relation to the Product(s) and Service(s) supplied to Customer under the Agreement. If a Privacy Data Sheet is attached to or referenced in this MDPA, this MDPA only refers to Cisco's role as a Processor as detailed in the respective Privacy Data Sheet, unless the Parties have explicitly agreed otherwise herein.

1.18. **"Processing"** means any operation or set of operations that is performed upon Personal Data, whether or not by automatic means, such as collection, recording, securing, organization, storage, adaptation or alteration, access to, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction. "**Processes**" and "**Process**" shall be construed accordingly.

1.19. **"Processor"** means an entity that processes Personal Data on behalf of a Controller. It shall have the same meaning ascribed to "processor" under the GDPR and other equivalent terms under other Data Protection Laws (e.g.: "Service Provider" as defined under the CCPA), as applicable.

1.20. **"Product"** means Cisco branded hardware and software offerings acquired by Customer.

1.21. **"Representatives"** means either Party's (including its Affiliates') officers, directors, employees, agents, contractors, temporary personnel, subcontractors and consultants.

1.22. **"Security Measures"** means the technical and organizational measures designed to protect the Personal Data as set forth in Cisco's Information Security Exhibit.

1.23. **"Service"** means Cisco branded service offering acquired by Customer.

1.24. **"Subprocessor"** means another Processor engaged by Cisco to carry out Processing of Customer's Personal Data, as set forth in the applicable Privacy Data Sheet(s).

2. Obligations of the Parties

2.1. The Parties agree that, for this MDPA, Customer shall be the Controller and Cisco shall be the Processor.

2.2. Customer shall:

a. use the Products and/or Services in compliance with Data Protection Laws;

b. ensure all instructions given by it to Cisco in respect of the Processing of Personal Data are at all times in accordance with Data Protection Laws;

c. ensure all Personal Data provided to Cisco has been collected in accordance with Data Protection Laws and that Customer has all authorizations and/or consents necessary to provide such Personal Data to Cisco; and

d. keep the amount of Personal Data provided to Cisco to the minimum necessary for the provision of the Products and/or Services.

2.3. Cisco shall:

a. only Process the Personal Data in accordance with Data Protection Laws and Customer's documented instructions, the applicable Privacy Data Sheet(s), Annex 1 to the EU Standard Contractual Clauses (where applicable), the Security Measures and this MDPA. Cisco will promptly notify Customer if Cisco reasonably believes that Customer's instructions are inconsistent with Data Protection Laws;

b. ensure its applicable Representatives who may Process Personal Data have written contractual obligations in place with Cisco to keep the Personal Data confidential or are under an appropriate statutory obligation of confidentiality;

c. appoint data protection lead(s). Upon request, Cisco will provide the contact details of the appointed person(s);

d. assist Customer as reasonably needed to respond to requests from supervisory authorities, Data Subjects, customers, or others to provide information related to Cisco's Processing of Personal Data;

e. if required by Data Protection Laws, court order, subpoena, or other legal or judicial process to Process Personal Data other than in accordance with Customer's instructions, notify Customer without undue delay of any such requirement before Processing the Personal Data (unless mandatory applicable law prohibits such notification, in particular on important grounds of public interest);

f. where Customer is acting as a Processor, act as a subprocessor of Customer;

g. maintain records of the Processing of any Personal Data received from Customer under the Agreement;

h. not lease, sell, distribute, or otherwise encumber Personal Data unless mutually agreed to by the Parties in a separate agreement;

i. not combine Personal Data received from or on behalf of Customer and Personal Data collected by Cisco's own interactions with the Data Subject other than as provided in the Agreement or as otherwise permitted by Data Protection Laws;

j. provide such assistance as Customer reasonably requires (either on its own behalf or on behalf of its customers), and Cisco or a Representative is able to provide, in order to meet any applicable filing, approval or similar requirements in relation to Data Protection Laws;

k. provide such information and assistance as Customer reasonably requires (taking into account the nature of Processing and the information available to Cisco) to enable compliance by Customer with its obligations under Data Protection Laws with respect to:

   i. security of Processing;

   ii. data protection impact assessments (as such term is defined by the GDPR);

   iii. prior consultation with a supervisory authority regarding high-risk Processing; and

   iv. notifications to the applicable supervisory authority and/or communications to Data Subjects by Customer in response to any Data Breach;

l. on termination of the MDPA for whatever reason, cease to Process Personal Data, and upon Customer's written request and without undue delay, (i) return, or make available for return, Personal Data in its possession or control, or (ii) securely delete or permanently render unreadable or inaccessible existing copies of the Personal Data; unless continued retention and Processing is required or is permitted by Data Protection Laws and/or mandatory applicable law. At Customer's request, Cisco shall give Customer confirmation in writing that it has fully complied with this Section 2.3 (k.iv) or provide a justification as to why such compliance is not feasible.

3. Transfers of Personal Data

Cisco may transfer and process Personal Data to and in locations where Cisco or its Subprocessors maintain Data Processing operations to provide the Products/Services as further detailed in the respective Privacy Data Sheet(s).

3.1. Transfers of Personal Data from the EEA or Switzerland to the US. Where Cisco Processes Personal Data from the EEA or Switzerland on behalf of Customer in the US, Cisco shall perform such Processing in accordance with the EU-US Data Privacy Framework or Swiss-US Data Privacy Framework, respectively, and in accordance with the EU Standard Contractual Clauses, as further detailed in Sections 3.3 and 3.5 below.

3.2. Transfers of Personal Data from the UK to the US. Where Cisco Processes Personal Data from the UK on behalf of Customer in the US, Cisco shall perform such Processing in accordance the UK Extension to the EU-US Data Privacy Framework and the EU Standard Contractual Clauses, as further detailed in Section 3.4 below.

3.3. Transfers of Personal Data from EEA to third countries. Where Cisco Processes Personal Data from the EEA on behalf of Customer in a country which is not an Approved Jurisdiction, Cisco shall perform such Processing in accordance with the EU Standard Contractual Clauses and/or in accordance with Articles 44 to 49 GDPR.

3.4. Transfers of Personal Data from the UK to third countries. Where Cisco Processes Personal Data from the UK in a third country, such Processing shall be performed in accordance with the EU Standard Contractual Clauses, as amended by the UK International Data Transfer Addendum to the EU Standard Contractual Clauses (the **"UK Addendum"**).

3.5. Transfers of Personal Data from Switzerland to third countries. Where Cisco Processes Personal Data from Switzerland in a third country, such Processing shall be performed in accordance with the EU Standard Contractual Clauses, as amended by the Swiss Addendum to the EU Standard Contractual Clauses (the "**Swiss Addendum**").

3.6. Transfers of Personal Data from jurisdictions other than the EEA, UK or Switzerland to third countries. For jurisdictions other than the EEA, UK or Switzerland, Cisco shall not transfer Personal Data outside of the jurisdiction where the Personal Data is obtained unless permitted under Data Protection Laws or instructed by Customer. Where Cisco Processes Personal Data from an APEC Member Economy on behalf of Customer, Cisco shall perform such Processing in a manner consistent with the APEC Cross Border Privacy Rules Systems requirements ("**CBPRs**") (see www.cbprs.org) to the extent the requirements are applicable to Cisco's Processing of the Personal Data. If Cisco is unable to provide the same level of protection as required by the CBPRs, Cisco shall promptly notify Customer and cease Processing. In such event, Customer may terminate the Agreement with respect only to those Products and/or Services for which Cisco is unable to provide the same level of protection as required by the CBPRs by written notice within 30 days.

Any further changes to the transfer mechanisms referred to in this Section 3 approved with an official decision by the applicable competent authority will be incorporated by reference and a copy of the new transfer mechanism will be available on the Cisco Trust Center.

4. Subprocessing

4.1. Where Cisco appoints a Subprocessor, Cisco will execute a written agreement with the Subprocessor containing terms at least as protective as this MDPA. Current Subprocessor(s) are listed in the applicable Privacy Data Sheet(s).

4.2. Cisco shall not subcontract its obligations under this MDPA to new Subprocessors, in whole or in part, without providing Customer with notice (e.g.: by publishing this information at Cisco's Trust Portal and/or by email upon Customer subscription at Cisco's Trust Portal) and an opportunity to object. If within 10 days of Cisco's notice, Customer objects to the proposed subcontracting by providing reasonable grounds related to the protection of the Personal Data and the Parties cannot resolve the objection within 30 days of Cisco's notice, then Customer may on written notice, terminate the applicable part of the Agreement and/or purchase order relating to those Products and/or Services which cannot be provided by Cisco without the use of the Subprocessor(s) giving rise to the objection.

4.3. Cisco shall be liable for the acts or omissions of Subprocessors to the same extent it is liable for its own actions or omissions under this MDPA.

4.4. For the purposes of Clause 9 of the EU Standard Contractual Clauses, Customer provides a general authorization to Cisco to engage Subprocessors. Such consent is conditional on Cisco's compliance with this Section 4.

5. Rights of Data Subjects

Data Subject requests. To the extent legally permitted, Cisco shall promptly redirect the Data Subjects to send their requests to Customer or notify Customer if it receives a Data Subject request for access to, rectification, portability, objection, restriction or erasure of such Data Subject's Personal Data. Unless required by Data Protection Laws, Cisco shall not respond to any such Data Subject request without Customer's prior written consent except to redirect the Data Subject request to Customer. Cisco shall provide such information and cooperation and take such action as Customer reasonably requests in relation to a Data Subject request.

6. Security

Controls for the Protection of Personal Data. Cisco shall implement and maintain the Security Measures and regularly monitor compliance with these Security Measures.

7. Audit

7.1. Cisco shall make available to Customer such information as is reasonably necessary to demonstrate Cisco's compliance with the obligations of this MDPA in accordance with the Security Measures.

7.2. Customer acknowledges and agrees that any exercise of its audit rights under Clause 8.9 of the EU Standard Contractual Clauses will be conducted in accordance with this MDPA.

8. Notification and Communication

8.1. Notification. Cisco shall notify Customer within 48 hours of confirmation of a Data Breach relating to Customer's Personal Data. Cisco shall provide all such timely information and cooperation as Customer may reasonably require for Customer to fulfil its Data Breach reporting obligations under (and in accordance with the timescales required by) Data Protection Law. Cisco shall further take such measures and actions as it considers necessary or appropriate to remedy or mitigate the effects of the Data Breach and shall keep Customer informed in connection with the Data Breach.

8.2. Information Security Communication. Except as required by mandatory applicable law, Cisco agrees that it will not inform any third party of a Data Breach referencing or identifying Customer, without Customer's prior written consent. Cisco shall reasonably cooperate with Customer and law enforcement authorities concerning a Data Breach. Cisco shall retain, for an appropriate period of time, all information and data within Cisco's possession or control that is directly related to any Data Breach. If disclosure of the Data Breach referencing or identifying Customer is required by mandatory applicable law, Cisco will work with Customer regarding the timing, content, and recipients of such disclosure.

8.3. Post-incident. Cisco shall reasonably cooperate with Customer in any post-incident investigation, remediation, and communication efforts.

8.4. Complaints or notices related to Personal Data. If Cisco receives any official complaint, notice, or communication that relates to Cisco's Processing of Personal Data or either Party's compliance with Data Protection Laws in connection with Personal Data, to the extent legally permitted, Cisco shall promptly notify Customer and, to the extent applicable, Cisco shall provide Customer with commercially reasonable cooperation and assistance in relation to any such complaint, notice, or communication.

9. General

9.1. Each Party's respective direct liability to data subjects or applicable supervisory data protection authorities which cannot be limited or excluded by mandatory applicable law shall be unlimited.

9.2. Except for any liability which cannot be limited or excluded under mandatory applicable law, the aggregate liability of Cisco for all Data Breaches and any breach of this MDPA (whether for breach of contract, misrepresentations, negligence, strict liability, other torts or otherwise) shall not exceed US$1,000,000.

9.3. Where a Data Breach and/or breach of this MDPA is also a breach of any confidentiality or non-disclosure obligations in the Agreement, the liability cap in Section 9.2 will apply.

9.4. No one other than a Party to this MDPA, their successors and permitted assignees shall have any right to enforce any of its terms.

9.5. This MDPA will remain in force for the term of Agreement.

Attachment A

EU Standard Contractual Clauses

Parties agree to incorporate Module 2 (Controller to Processor) and Module 3 (Processor to Processor) of the EU Standard Contractual Clauses to this MDPA. Where Customer acts as a Controller and Cisco is the Processor, Module 2 of the EU Standard Contractual Clauses applies. Where Customer acts as a Processor and Cisco is a subprocessor, Module 3 of the EU Standard Contractual Clauses applies. In both scenarios, the EU Standard Contractual Clauses will apply subject to the following understandings:

i. Clause 7 ("Docking Clause") applies.

ii. Clause 9: Option 2 applies. Customer gives Cisco general written authorization to engage subprocessors. Cisco shall inform Customer in writing of any intended changes through the addition or replacement of subprocessors at least 30 days in advance.

iii. Clause 11 (a): The option to lodge a complaint with an independent dispute resolution body does not apply.

iv. Clause 17: The governing law shall be the law of the Netherlands.

v. Clause 18: Any dispute arising from the EU Standard Contractual Clauses shall be resolved by the courts of the Netherlands.

Annex 1 to the EU Standard Contractual Clauses

Customer can subscribe on Cisco's Trust Portal to receive email notifications with detailed information about any updates to the processing operations of Cisco Product and Services published in the applicable Privacy Data Sheet(s). By clicking on the "Subscribe" link located in the upper right-hand corner of the Privacy Data Sheet(s), Customer will receive an email notification when the Privacy Data Sheet(s) to which Customer has subscribed are updated.

A. List of Parties

Data exporter

The data exporter is Customer, acting as data exporter on behalf of itself or a customer where applicable. Activities relevant to the transfer include the performance of services for Customer and its customer(s).

Data importer

The data importer is Cisco. Activities relevant to the transfer include the performance of services for Customer and its customer(s).

B. Description of transfer

1. Categories of data subjects whose personal data is transferred

The personal data transferred may concern the following categories of data subjects: employees, contractors, business partners, representatives and end customers of the Customer, and other individuals whose personal data is processed by or on behalf of Customer or Customer's customers and delivered as part of the Services and Products.

2. Categories of personal data transferred

The personal data transferred may concern the following categories of data:

Personal data related directly or indirectly to the categories of data subjects listed above, including online and offline customer, prospect, and partner data, and personal data provided by or on behalf of the Customer or its users of the Services and Products. More detailed categories of personal data are reflected for certain Services and Products in Cisco's Privacy Data Sheets available at https://trustportal.cisco.com.

3. Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

Unless data exporter or its users use data importer's products and services to transmit or store sensitive data, data importer does not process sensitive data.

4. The frequency of the transfer (e.g.: whether the data is transferred on a one-off or continuous basis).

The transfer happens on a continuous basis.

5. Nature of Processing

Personal data will be subject to processing activities such as storing, recording, using, sharing, transmitting, analyzing, collecting, transferring, and making available personal data. More details on Cisco's processing activities of personal data are reflected for certain Services and Products in Cisco's Privacy Data Sheets available at https://trustportal.cisco.com.

6. Purpose(s) of the data transfer and further processing

The personal data transferred may be subject to the following basic processing activities, as may be further set forth in contractual agreements entered into from time to time between Cisco and Customer: (a) customer service activities, such as processing orders, providing technical support and improving offerings, (b) sales and marketing activities as permissible under mandatory applicable law, (c) consulting, professional, security, storage, hosting and other services delivered to Customer, and (d) internal business processes and management, fraud detection and prevention, and compliance with governmental, legislative, and regulatory requirements. More detailed purposes for Cisco's processing of personal data are reflected for certain Services and Products in Cisco's Privacy Data Sheets available at https://trustportal.cisco.com.

7. The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Personal data will be retained as needed to fulfill the purposes for which it was collected, such as delivery of the Services and Products, and as necessary for Cisco to comply with its business requirements, legal obligations, resolve disputes, protect its assets, and enforce its rights and agreements.

Specific data retention periods for Cisco's processing of personal data are reflected for certain Services and Products in Cisco's Privacy Data Sheets available at https://trustportal.cisco.com.

8. For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Personal data will be transferred to Cisco's sub-processors for certain Services and Products as described in Cisco's Privacy Data Sheets available at https://trustportal.cisco.com.

C. Competent Supervisory Authority

Identify the competent supervisory authority/ies in accordance with Clause 13:

It is competent supervisory authority/ies in accordance with Clause 13 with responsibility for ensuring compliance by the data exporter.

Annex 2 to the EU Standard Contractual Clauses

Annex 2 to the EU Standard Contractual Clauses is the Security Measures.

Further up-to-date Product and/or Service specific technical and organisational measures will be set out in the applicable Cisco Privacy Data Sheets and Product and/or Service-related certifications published on Cisco's Trust Portal at https://trustportal.cisco.com/.

Annex 3 to the EU Standard Contractual Clauses

The controller has authorised the use of the sub-processors listed in the applicable Cisco Privacy Data Sheet published on Cisco's Trust Portal at https://trustportal.cisco.com/c/r/ctp/trust-portal.html?doctype=Privacy%20Data%20Sheet|Privacy%20Data%20Map.

Customer can subscribe to receive email notifications with detailed information about any updates to the processing operations of Cisco Product and Services published in the applicable Privacy Data Sheet(s), including also changes to the engaged Subprocessors. By clicking on the "Subscribe" link located in the upper right-hand corner of the Privacy Data Sheet(s), Customer will receive an email notification when the Privacy Data Sheet(s) to which Customer has subscribed are updated.